

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No. 09/507,191
Filing Date February 18, 2000
Confirmation No. 8393
Assignee Microsoft Corporation
Inventorship ENGLAND, Paul
Group Art Unit 2136
Examiner Colin, Carl G.
Attorney's Docket No. MS1-0408US
Title: VERIFYING THE PRESENCE OF AN ORIGINAL DATA STORAGE MEDIUM

APPEAL BRIEF

To: Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

From: Rich Bucher (Tel. 509-324-9256x216; Fax 509-323-8979)
Customer No. 22801

Pursuant to 37 C.F.R. §41.37, Applicant hereby submits an appeal brief for application 09/507,191, filed February 18, 2000, within the requisite time from the date of filing the Notice of Appeal. Accordingly, Applicant appeals to the Board of Patent Appeals and Interferences seeking review of the Examiner's rejections.

<u>Appeal Brief Items</u>	<u>Page</u>
(1) Real Party in Interest	3
(2) Related Appeals and Interferences	3
(3) Status of Claims	3
(4) Status of Amendments	3
(5) Summary of Claimed Subject Matter	3
(6) Grounds of Rejection to be Reviewed on Appeal	6
(7) Argument	6
(8) Appendix of Appealed Claims	22
(9) Evidence appendix	27
(10) Related Proceedings appendix	28

(1) Real Party in Interest

The real party in interest is Microsoft Corporation, the assignee of all right, title and interest in and to the subject invention.

(2) Related Appeals and Interferences

Appellant is not aware of any other appeals, interferences, or judicial proceedings which will directly affect, be directly affected by, or otherwise have a bearing on the Board's decision to this pending appeal.

(3) Status of Claims

Claims 1-42 and 44 were previously canceled.

Claims 43 and 45-62 stand rejected and are pending in the Application. Claims 43 and 45-62 are set forth in the Appendix of Appealed Claims on page 22.

(4) Status of Amendments

The most recent final Office Action was mailed 05/23/2006. No claims have been amended subsequent to this final Office Action.

(5) Summary of Claimed Subject Matter

A concise explanation of each of the independent claims is included in this Summary section, including specific reference characters, if any. These specific reference characters are examples of particular elements of the drawings for certain embodiments of the claimed subject matter and the claims are not limited to solely the elements corresponding to these reference characters.

With regard to claim 43, a method comprising: randomly retrieving a plurality of blocks of data from a computer-readable media, wherein at least one block of data includes data not contained in a given content (Page 4 (lines 20-21), Page 9 (lines 10-15), Fig. 2 (122, 124), Page 13 (lines 11-12), Fig. 5 (222, 224)); generating a digest value for each of the plurality of randomly retrieved blocks of data (Page 9 (lines 15-17), Fig. 2 (126), Page 13 (lines 12-14), Fig. 5 (226)); comparing each of the digest values to a set of verification data (Page 10 (lines 8-10), Fig. 2 (128), Page 13 (lines 14-16), Fig. 5 (228)); determining that the computer-readable media contains an original version of the given content if the digest values match a subset of the verification data (Page 10 (lines 10-20), Fig. 2 (130, 134), Page 13 (lines 16-23), Fig. 5 (226)); and allowing access to a functionally equivalent version of the given content, which is smaller than the original version, if the digest values match a subset of the verification data (Page 6 (lines 10-15), Page 9 (lines 17-19), Page 10 (lines 15-17), Fig. 2 (136), Page 13 (lines 23-24), Fig. 5 (236)).

With regard to claim 50, a method comprising: receiving a request to access a given content (Page 9 (line 9), Fig. 2 (120), Page 13 (lines 9-11), Fig. 5 (220)); calculating a digest value for each of a set of blocks of data randomly retrieved from a computer-readable media, wherein at least one block of data includes data not contained in the given content (Page 9 (lines 15-17), Fig. 2 (126), Page 13 (lines 12-14), Fig. 5 (226)); verifying whether the received plurality of blocks are from an original version of the given content by comparing the calculated digest values to a set of associated verification digest values (Page 10 (lines 8-20), Fig. 2 (128, 130), Page 13 (lines 14-20), Fig. 5 (228, 230)); and controlling access to a

functionally equivalent version of the given content, which is smaller than the original version, if the calculated digest values match a subset of the associated verification digest values (Page 6 (lines 10-15), Page 9 (lines 17-19), Page 10 (lines 15-17), Fig. 2 (136), Page 13 (lines 23-24), Fig. 5 (236)).

With regard to claim 58, a verification system comprising: a data reading device to read data from a computer-readable media (Page 4 (lines 18-20), Page 13 (line 12)); and a verification module coupled to the data reading device (Page 4 (lines 18-20), Fig. 4, Fig. 6, Page 13 (line 12)), wherein the verification module is adapted to receive a request to access a given content (Page 9 (line 9), Fig. 2 (120), Page 13 (lines 9-11), Fig. 5 (220)), to request a random set of blocks of data from the computer-readable media that includes at least one block of data that does not contain the given content (Page 4 (lines 20-21), Page 9 (lines 10-15), Fig. 2 (122, 124), Page 13 (lines 11-12), Fig. 5 (222, 224)), to verify whether the received plurality of blocks are from an original version of the given content by comparing digest values of a received set of blocks of data to a corresponding set of known valid digest values (Page 10 (lines 8-20), Fig. 2 (128, 130), Page 13 (lines 14-20), Fig. 5 (228, 230)), and to control access to a functionally equivalent version of the given content, which is smaller than the original version, if the calculated digest values match a subset of the known valid digest values (Page 6 (lines 10-15), Page 9 (lines 17-19), Page 10 (lines 15-17), Fig. 2 (136), Page 13 (lines 23-24), Fig. 5 (236)).

(6) Grounds of Rejection to be Reviewed on Appeal

Claims 43 and 45-62 stand rejected under 35 U.S.C. §103(a) as being obvious over U.S. Patent No. 6,367,019 to Ansell et al. (hereinafter "Ansell") in view of U.S. Patent No. 5,745,678 to Herzberg (hereinafter "Herzberg").

(7) Argument

- A. The rejections under 35 U.S.C. §103(a) over Ansell and Herzberg fail because the Office has failed to establish a *prima facie* case of obviousness.

Applicant respectfully submits that the Office has not established a *prima facie* case of obviousness. The discussion below proceeds as follows. First, a section entitled "The § 103 Standard" is provided which describes the criteria that must be met in order to establish a *prima facie* case of obviousness. Second, a section entitled "The Claims" is provided which presents Applicant's reasoning as to why the Office has not met these criteria.

The §103 Standard

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, *there must be some suggestion or motivation*, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, *to modify the reference or to combine reference teachings*. Second, there must be a reasonable expectation of success. Finally, *the prior art reference (or references when combined) must teach or suggest all the claim limitations*. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on

Applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

The Claims

Claim 43 recites a method comprising:

- randomly retrieving a plurality of blocks of data from a computer-readable media, wherein at least one block of data includes data not contained in a given content;
- generating a digest value for each of the plurality of randomly retrieved blocks of data;
- comparing each of the digest values to a set of verification data;
- determining that the computer-readable media contains an original version of the given content if the digest values match a subset of the verification data; and
- allowing access to a functionally equivalent version of the given content, which is smaller than the original version, if the digest values match a subset of the verification data.

In making out the rejection of this claim, the Office argues that its subject matter is rendered obvious in view of Ansell and Herzberg. Specifically, the Office argues that Ansell discloses most of the subject matter of this claim, but is silent as to the term “random” as it pertains to retrieving data. For this subject matter, the Office relies on Herzberg and argues that it teaches randomly retrieving data to determine if data is valid – which helps reduce the possibility of forgery. The Office then argues that it would have been obvious to modify “the method of retrieving portion of data to be validated for execution” of Ansell with the “randomly retrieving selecting portion” of Herzberg. As a motivation for the suggested combination, the Office states that such motivation would be “in order to more efficiently validate the multimedia program because the random selection

helps reduce the possibility of forgery as the checking may be based on part of the data”.

Applicant respectfully disagrees and submits that the Office has not established a *prima facie* case of obviousness.

First, Applicant submits that the references do not collectively disclose all of the subject matter of this claim. Specifically, the Office relies on the individual component keys (Keys 506A1-4) of Ansell (see Columns 7 and 8) - which together comprise storage key 504A - as disclosing “a plurality of blocks of data”, as claimed. This is confirmed by the fact that the Office relies on the forming of a digest for each of these individual component keys as disclosing “generating a digest value for each of the plurality of randomly retrieved blocks of data”, as claimed. However, the Office appears to forget that the storage key 504A and its individual component keys are not retrieved “from a computer-readable media”. Instead, they are integrated into the player itself, each particular storage key being unique to its corresponding player (e.g., see Abstract, Column 6 (lines 34-40)). In fact, each player’s key is difficult to change, “typically requiring physical deconstruction” of the portable player. (see Column 6 (line 40)). As such, Ansell cannot possibly disclose “randomly retrieving a plurality of blocks of data *from a computer-readable media*”, as claimed. (emphasis added).

What’s more, in Ansell, only *one digest value for a single individual component key* is used with respect to storage key field 406 in the header of the SPT. (see Column 6 (line 49)). As such, even if Ansell did teach “randomly *retrieving* a plurality of blocks of data” and “generating a digest value *for each...*”, which it does not, it cannot possibly disclose “determining that the

computer-readable media contains an original version of the given content if the digest values match a subset of the verification data” or “allowing access... if the digest values match a subset of the verification data.” (emphasis added).

Furthermore, Ansell simply fails to disclose or suggest “allowing access to a functionally equivalent version of the given content, which is smaller than the original version”, as claimed. The Office argues that at least part of this feature is disclosed in Column 11 (lines 10-55). However, this portion of Ansell merely discloses that “tracks 112 can have **restrictions** placed upon them” such as “the number of times SPT 116 can be played back, an expiration time beyond which SPT 116 cannot be played back, a number of storage media such as storage medium 202 (FIG. 2) on which SPT 116 can be fixed, and the number of devices to which SPT 116 can be bound.” Applicant fails to see how this discloses “smaller than the original version”, as that term is used and understood in the context of the subject application (by way of example and not limitation, see Page 6 (lines 10-15) of the subject application).

Second, Applicant submits that Herzberg fails to disclose or suggest “randomly retrieving a plurality of blocks of data”, as claimed. Instead, it describes a system for detecting authorized multimedia programs, which includes “creat[ing] a validation structure for validating a multimedia program,” “embed[ding] the validation structure in the multimedia program,” and determining “whether the multimedia program is an authorized multimedia program” using the validation structure (see Column 1 (lines 52-60)). Herzberg goes on to describe on Columns 1 (line 61) through 2 (line 14) that (emphasis added):

...sections of the program (hereinafter called data objects) are selected and a cryptographic hash value is created or calculated on each of the selected data objects. The cryptographic hash value and the location of the selected data object are stored as a data record within the validation structure

Determining whether a multimedia program is an authorized multimedia program is accomplished by selecting a subset of the data objects within the multimedia program and validating the selected data objects using the validation structure stored in the multimedia program. This includes the steps of randomly selecting a portion of the data objects *from among a defined set of data records* listed in the validation structure, reading the selected data objects from the multimedia program using location information stored in the validation structure, and validating the selected data objects using validation information stored in the validation structure.

As this excerpt makes clear, Herzberg teaches *pre-selecting sections* of a program for use in the validating structure and randomly selecting data objects only *from the pre-selected sections* of the program specified in the validation structure. Thus, the selected data objects of Herzberg cannot be equated with “a plurality of blocks” that are *randomly retrieved “from a computer-readable media”*, as claimed.

Third, Applicant submits that the Office’s stated motivation – that of improving efficiency – is too general and lacks the particularity that is required when making out a *prima facie* case of obviousness. See, e.g., *In re Kotzab*, 217 F.3d 1365, 1371, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000) (“particular findings must be made as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed”).

In this regard, the Office itself has provided a paper, available at the following link:

<http://www.uspto.gov/web/menu/busmethp/busmeth103rej.htm>

that describes proper and improper rejections made under §103(a). Particularly instructive is Example 17 that appears in Section V of the paper illustrating an improper §103(a) rejection which is based upon a proposed motivation that is simply too general and lacking in particularity. This example is reproduced below in its entirety for the Office's convenience:

V. Examples of Improper Rejection under 35 U.S.C. 103

Example 17: Improper rejection based upon hindsight - general motivation statement.

a. The claimed invention

The invention is drawn to a smart card containing a tracking mechanism, which tracks shopping preferences of consumers by recording the type, quantity, and dates of purchase for a pre-selected group of products. The smart card is useful in a system and method for introducing new and alternative products that are of the same type as products normally purchased by the shopper. The smart card records the shopper's purchases and submits an automatic notification to the shopper when a quantity threshold is achieved for the pre-selected products. This notification will encourage the consumer to consider alternative products by providing the consumer incentives, such as a pricing discount, to purchase an alternative product.

Claim 1:

A method for using a smart card in a marketing analysis program designed to introduce new products, the method comprising the steps of:

storing product information on the smart card when said products are purchased by a consumer wherein said information including type, quantity and dates of the product purchased;

identifying for each product a threshold for each of said type, quantity and dates of products purchased;

determining an incentive for an alternative product based on said threshold; and

automatically notifying said consumer when said threshold is reached for a given product identified on the smart card and providing the consumer with said incentive, whereby the incentive encourages the consumer to consider alternative products.

b. Evidence

Reference A discloses smart card that tracks consumer preferences by recording the type, quantity, and dates of purchase of pre-selected products to determine trends in consumer purchases. The smart card is periodically read by a scanner to determine its contents for market analysis. In return for using the smart card and participating in the marketing program, the user is provided with free product coupons for products that are normally purchased by the shopper.

Reference B discloses a traditional consumer incentive program that provides coupons for the purchase of named products based upon the consumer's purchase of those same products to promote customer loyalty.

c. Poor statement of the rejection

Claim 1 is rejected under 35 U.S.C. 103 as being unpatentable over Reference A in view of Reference B. Reference A discloses the conventional use of a smart card to track consumer preferences and provide incentives. However, Reference A does not disclose the automatic notification to consumer providing incentives. Reference B discloses providing incentives to consumers to purchase the desired products. *It would have been obvious to combine Reference A's smart card with Reference B's incentive to consumers because the combination would allow Reference A's smart card to be more efficient.*

d. Analysis

The motivation, improve efficiency, is too general because it could cover almost any alteration contemplated of Reference A and does not address why this specific proposed modification would have been obvious. Additionally, there is nothing in either of references that would suggest automatically notifying the consumer when reaching a threshold nor is there anything in either reference that would suggest the notifying step. Finally, although Reference B teaches a traditional coupon scheme to promote customer loyalty, there is no suggestion, other than applicant's disclosure, to employ this scheme to promote the introduction of new and alternative products. *The rejection is improper.*

Accordingly, as this example illustrates, the Office's stated motivation of improving efficiency is improper because it is too general and could cover almost any alteration contemplated of Ansell.

Fourth and perhaps most importantly, even if the Office's stated motivation was not too general, which it is, there can still be no motivation to combine these references because modifying Ansell with the teachings of Herzberg would impermissibly change Ansell's principle of operation and impermissibly render it unsatisfactory for its intended purpose. (see MPEP 2143). Specifically, after the logic of Ansell selectively retrieves "read-only serial number 204 from storage media and media identification data from media identification field 402", it selects "either read-only key 505A or a selected one of component keys 506A1-4 according to the digest stored in storage key field 406". (see Fig. 7 (steps 702 and 704) and Column 8 (lines 19-58)). This selectivity is necessary because the player logic forms digests of each component key (506AA1-4) of key 504A and then "selects the one of keys 504A, 506AA1-4 whose digest is accurately represented in storage key identification field 406". (Column 8 (lines 49-50)). Only after/if

the appropriate component key is identified can the media master key, and thus the content of SPT 116, be decrypted.

In this way, Ansell's very operation depends on selecting specific key(s) from the storage media. Accordingly, if Ansell's logic was modified so that data blocks were retrieved randomly, as suggested by the Office, the appropriate keys would rarely, if ever, be available to form digests and the content of SPT would therefore not be decrypted. Thus, Ansell's principle of operation, as illustrated in the logic flow diagram of Fig. 7, would be changed such that it would be rendered unsatisfactory for its intended purpose of providing the owner "reasonable unimpeded convenience of use and enjoyment of the content." (see Column 2 (lines 1-3)).

In view of the above discussion, the Office has not established a *prima facie* case of obviousness. Accordingly, for at least this reason, this claim is allowable.

Claims 45-49 depend from claim 43 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 43, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

In addition, regarding claim 45, the Office argues that Columns 8 (lines 45-67), 21 (lines 52-57) and 5 (lines 1-18) teach "allowing access to related material if the digest values match a subset of the verification data." However, after reviewing these excerpts, Applicant is unable to find any discussion or suggestion

of this subject matter. Therefore, Applicant can only conclude that the Office's reliance on these excerpts is misplaced.

In addition, regarding claim 46, the Office does not specifically address the subject matter of this claim. Nevertheless, Applicant has thoroughly searched the cited references and is unable to find any disclosure or suggestion wherein "generating the digest value...comprises calculating a cryptographic hash value." Accordingly, Applicant submits that the Office's reliance on these references is misplaced.

Claim 50 recites a method comprising:

- receiving a request to access a given content;
- calculating a digest value for each of a set of blocks of data randomly retrieved from a computer-readable media, wherein at least one block of data includes data not contained in the given content;
- verifying whether the received plurality of blocks are from an original version of the given content by comparing the calculated digest values to a set of associated verification digest values; and
- controlling access to a functionally equivalent version of the given content, which is smaller than the original version, if the calculated digest values match a subset of the associated verification digest values.

In making out the rejection of this claim, the Office argues that its subject matter is rendered obvious in view of Ansell and Herzberg. Specifically, the Office argues that Ansell discloses most of the subject matter of this claim, but is silent as to the term "random" as it pertains to retrieving data. For this subject matter, the Office relies on Herzberg and argues that it teaches randomly retrieving data to determine if data is valid – which helps reduce the possibility of

forgery. The Office then argues that it would have been obvious to modify “the method of retrieving portion of data to be validated for execution” of Ansell with the “randomly retrieving selecting portion” of Herzberg. As a motivation for the suggested combination, the Office states that such motivation would be “in order to more efficiently validate the multimedia program because the random selection helps reduce the possibility of forgery as the checking may be based on part of the data”.

Applicant respectfully disagrees and submits that the Office has not established a *prima facie* case of obviousness.

First, Applicant submits that the references do not collectively disclose all of the subject matter of this claim. Specifically, as noted above, the storage key 504A (and its individual component keys) in Ansell is not retrieved “from a computer-readable media”. Instead, it is integrated into the player itself, each particular storage key being unique to its corresponding player. What’s more, in Ansell, only *one digest value* for a *single individual component key* is used with respect to storage key field 406 in the header of the SPT. As such, Ansell cannot possibly disclose “verifying whether the received plurality of blocks are from an original version”, as claimed or “controlling access...if the calculated digest values match a subset of the associated verification digest values. (emphasis added). Furthermore, Ansell simply fails to disclose or suggest “controlling access to a functionally equivalent version of the given content, *which is smaller than the original version*”, as claimed. (emphasis added).

Second, as discussed above, the data objects of Herzberg are selected only from *pre-selected sections* and thus cannot be equated with “set of blocks of data randomly retrieved from a computer-readable media”, as claimed.

Third, as illustrated by the Office’s own example, the Office’s stated motivation – that of improving efficiency – is too general because it could cover almost any alteration contemplated of Ansell.

Fourth and perhaps most importantly, even if the Office’s stated motivation was not too general, which it is, there can still be no motivation to combine these references because modifying Ansell in the proposed manner would impermissibly change its principle of operation and impermissibly render it unsatisfactory for its intended purpose.

In view of the above discussion, the Office has not established a *prima facie* case of obviousness. Accordingly, for at least this reason, this claim is allowable.

Claims 51-57 depend from claim 50 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 50, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

In addition, regarding claims 52-53, the Office argues that Columns 8 (lines 45-67), 21 (lines 52-57) and 5 (lines 1-18) teach “allowing access to related material if the digest values match a subset of the verification data.” However, after reviewing these excerpts, Applicant is unable to find any discussion or

suggestion of this subject matter. Therefore, Applicant can only conclude that the Office's reliance on these excerpts is misplaced.

In addition, regarding claim 54, Applicant fails to see where Column 10 (lines 38-58) of *Hertzberg* even suggests that "a set of digest values" (which, the Office argues *Ansell* discloses on Columns 7 and 8) "are stored with the original version of the given content." Instead, as far as Applicant can discern, this excerpt from Herzberg merely describes a process by which a token generation module generates signature tokens. Nor has the Office provided any explanation other than merely referring to this excerpt. Therefore, Applicant can only conclude that the Office's reliance on this excerpt is misplaced.

Claim 58 recites a verification system comprising:

- a data reading device to read data from a computer-readable media; and
- a verification module coupled to the data reading device, wherein the verification module is adapted to receive a request to access a given content, to request a random set of blocks of data from the computer-readable media that includes at least one block of data that does not contain the given content, to verify whether the received plurality of blocks are from an original version of the given content by comparing digest values of a received set of blocks of data to a corresponding set of known valid digest values, and to control access to a functionally equivalent version of the given content, which is smaller than the original version, if the calculated digest values match a subset of the known valid digest values.

In making out the rejection of this claim, the Office argues that its subject matter is rendered obvious in view of *Ansell* and *Herzberg*. Specifically, the Office argues that *Ansell* discloses most of the subject matter of this claim, but is silent as to the term "random" as it pertains to retrieving data. For this subject

matter, the Office relies on Herzberg and argues that it teaches randomly retrieving data to determine if data is valid – which helps reduce the possibility of forgery. The Office then argues that it would have been obvious to modify “the method of retrieving portion of data to be validated for execution” of Ansell with the “randomly retrieving selecting portion” of Herzberg. As a motivation for the suggested combination, the Office states that such motivation would be “in order to more efficiently validate the multimedia program because the random selection helps reduce the possibility of forgery as the checking may be based on part of the data”.

Applicant respectfully disagrees and submits that the Office has not established a *prima facie* case of obviousness.

First, Applicant submits that the references do not collectively disclose all of the subject matter of this claim. Specifically, as noted above, the storage key 504A (and its individual component keys) in Ansell is not retrieved from any computer-readable media. Instead, it is integrated into the player itself, each particular storage key being unique to its corresponding player. What’s more, in Ansell, only *one digest value* for a *single individual component key* is used with respect to storage key field 406 in the header of the SPT. As such, Ansell cannot possibly disclose “to verify whether the received plurality of blocks are from an original version”, as claimed or “to control access...if the calculated digest values match a subset of the known valid digest values. (emphasis added). Furthermore, Ansell simply fails to disclose or suggest “to control access to a functionally equivalent version of the given content, *which is smaller than the original version*”, as claimed. (emphasis added).

Second, as discussed above, the data objects of Herzberg are selected only from *pre-selected sections* and thus cannot be equated with “a random set of blocks of data from the computer-readable media”, as claimed.

Third, as illustrated by the Office’s own example, the Office’s stated motivation – that of improving efficiency – is too general because it could cover almost any alteration contemplated of Ansell.

Fourth and perhaps most importantly, even if the Office’s stated motivation was not too general, which it is, there can still be no motivation to combine these references because modifying Ansell in the proposed manner would impermissibly change its principle of operation and impermissibly render it unsatisfactory for its intended purpose.

In view of the above discussion, the Office has not established a *prima facie* case of obviousness. Accordingly, for at least this reason, this claim is allowable.

Claims 59-62 depend from claim 58 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 58, are neither disclosed nor suggested in the references of record, either singly or in combination with one another.

In addition, regarding claim 59, the Office argues that Columns 8 (lines 45-67), 21 (lines 52-57) and 5 (lines 1-18) teach “allowing access to related material if the digest values match a subset of the verification data.” However, after reviewing these excerpts, Applicant is unable to find any discussion or suggestion

of this subject matter. Therefore, Applicant can only conclude that the Office's reliance on these excerpts is misplaced.

In addition, regarding claim 61, the Office argues that Figs. 1 and 5 of Ansell teach "wherein the verification module is located in a server containing the corresponding set of known valid digest values and the data reading device is located in computer system coupled to the server." However, these figures only depict the player logic and storage keys as residing on the media player(s). Therefore, Applicant can only conclude that the Office's reliance on Ansell for this subject matter is misplaced.

Conclusion

The Office has failed to establish a *prima facie* case of obviousness. Accordingly, Applicant respectfully requests that the rejections be overturned and that the pending claims be allowed to issue.

Respectfully Submitted,

Dated: _____

10/8/06

By: _____

Rich Bucher
Lee & Hayes, PLLC
Reg. No. 57,971
(509) 324-9256 ext. 216

(8) Appendix of Appealed Claims

43. **(Previously Presented)** A method comprising:

randomly retrieving a plurality of blocks of data from a computer-readable media, wherein at least one block of data includes data not contained in a given content;

generating a digest value for each of the plurality of randomly retrieved blocks of data;

comparing each of the digest values to a set of verification data;

determining that the computer-readable media contains an original version of the given content if the digest values match a subset of the verification data; and

allowing access to a functionally equivalent version of the given content, which is smaller than the original version, if the digest values match a subset of the verification data.

45. **(Previously Presented)** A method according to Claim 43, further comprising allowing access to related material if the digest values match a subset of the verification data.

46. **(Previously Presented)** A method according to Claim 43, wherein generating the digest value for each of the plurality of randomly retrieved blocks of data comprises calculating a cryptographic hash value.

47. **(Previously Presented)** A method according to Claim 43, wherein the processes of randomly retrieving a plurality of blocks of data, generating digest values, comparing each of the digest values and determining that the computer-readable media contains an original version are performed when a watermark is embedded in the functionally equivalent version of the given content.

48. **(Previously Presented)** A method according to Claim 43, further comprising:

partitioning a trusted version of the first content into a plurality of verification data blocks; and

establishing the plurality of verification data by calculating a cryptographic hash value for each of the plurality of verification data blocks.

49. **(Previously Presented)** One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 43.

50. **(Previously Presented)** A method comprising:

receiving a request to access a given content;

calculating a digest value for each of a set of blocks of data randomly retrieved from a computer-readable media, wherein at least one block of data includes data not contained in the given content;

verifying whether the received plurality of blocks are from an original version of the given content by comparing the calculated digest values to a set of associated verification digest values; and

controlling access to a functionally equivalent version of the given content, which is smaller than the original version, if the calculated digest values match a subset of the associated verification digest values.

51. **(Previously Presented)** The method according to Claim 50, wherein controlling access to a functionally equivalent version of a given content comprises playing a requested music file if the calculated digest values match a subset of the associated verification digest values.

52. **(Previously Presented)** The method according to Claim 50, wherein controlling access to a functionally equivalent version of a given content comprises launching a requested application program if the calculated digest values match a subset of the associated verification digest values.

53. **(Previously Presented)** The method according to Claim 50, wherein controlling access to a functionally equivalent version of a given content comprises preventing installation of a requested music file if any of the calculated digest values do not match any associated digest value.

54. **(Previously Presented)** The method according to Claim 50, wherein the set of associated verification digest values are stored with the original version of the given content.

55. **(Previously Presented)** The method according to Claim 50, wherein the set of associated verification digest values are available on an internet web site.

56. **(Previously Presented)** The method according to Claim 50, further comprising verifying that the set of associated verification digest values come from a known authority.

57. **(Previously Presented)** One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 50.

58. **(Previously Presented)** A verification system comprising:
a data reading device to read data from a computer-readable media; and
a verification module coupled to the data reading device, wherein the verification module is adapted to receive a request to access a given content, to request a random set of blocks of data from the computer-readable media that includes at least one block of data that does not contain the given content, to verify whether the received plurality of blocks are from an original version of the given content by comparing digest values of a received set of blocks of data to a corresponding set of known valid digest values, and to control access to a

functionally equivalent version of the given content, which is smaller than the original version, if the calculated digest values match a subset of the known valid digest values.

59. **(Previously Presented)** A verification system as recited in Claim 58, wherein the verification module is further adapted to control access to related material if the calculated digest values match a subset of the known valid digest values.

60. **(Previously Presented)** A verification system as recited in Claim 58, wherein the verification module is located in a handheld audio player containing the functionally equivalent version of the given content and the data reading device is located in a computer system coupled to the handheld audio player.

61. **(Previously Presented)** A verification system as recited in Claim 58, wherein the verification module is located in a server containing the corresponding set of known valid digest values and the data reading device is located in computer system coupled to the server.

62. **(Previously Presented)** A verification system as recited in Claim 58, wherein the verification module and the data reading device are coupled to one another across the Internet.

(9) Evidence appendix. None

(10) Related proceedings appendix. None